# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-303947
(43)Date of publication of application : 13.11.1998

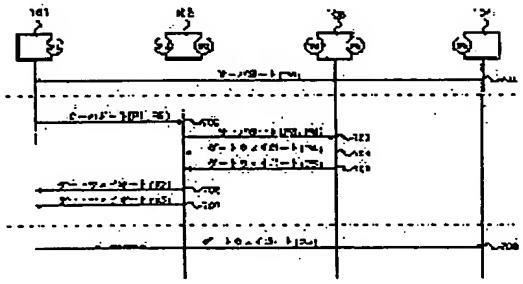
(51)Int.Cl. H04L 12/40
G06F 13/00
G06F 13/00
G06F 13/14

(21)Application number : 09-108839
(22)Date of filing : 25.04.1997

(71)Applicant : HITACHI LTD
(72)Inventor : KAYASHIMA MAKOTO
TERADA MASATOSHI
FUJIYAMA TATSUYA
KATOU ERI

## (54) NETWORK COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To normally exchange port numbers in a system in which communication is relayed by plural substitutive servers to individually constitute fire walls.
SOLUTION: Each of substitutive server computers 102, 103 interposed on a communication route between a client computer 101 and a server computer 104 and to individually constitute the fire walls is provided with a means to transfer a port number assigned by the server computer from the client computer 101 to the substitutive server computer to be connected with the server computer 104, a means to return the port number assigned by its own substitutive server computer according to transfer and a means to discriminate the port number returned from the substitutive server computer to be connected with the server computer and to transfer the port number to the client computer. The client computer 101 is provided with a means to exchange the port number of the server computer and the port number of the substitutive server computer to be connected with the server computer between the client computer 101 and the server computer.



LEGAL STATUS

[Date of request for examination] 14.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3354433
[Date of registration] 27.09.2002
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－303947

(43)公開日　平成10年(1998)11月13日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 12/40 | | Ｈ０４Ｌ | 11/00 | ３２１ |
| Ｇ０６Ｆ | 13/00 | ３５１ | Ｇ０６Ｆ | 13/00 | ３５１Ａ |
| | | ３５５ | | | ３５５ |
| | 13/14 | ３２０ | | 13/14 | ３２０Ｋ |

審査請求　未請求　請求項の数７　ＯＬ　（全 17 頁）

(21)出願番号　特願平9－108839

(22)出願日　平成９年(1997)４月25日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　萱島　信
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　藤山　達也
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　ネットワーク通信システム

(57)【要約】

【課題】　個別にファイアウォールを構成する複数の代理サーバにより通信が中継されるシステムにおいて、ポート番号の正常な交換を可能とする。

【解決手段】　クライアント計算機およびサーバ計算機間の通信経路に介在し、個別にファイアウォールを構成する複数の代理サーバ計算機の各々は、サーバ計算機の割り振ったポート番号を、クライアント計算機から、サーバ計算機に接続される代理サーバ計算機にかけて転送する手段と、当該転送に応じて、自代理サーバ計算機の割り振ったポート番号を返送する手段と、サーバ計算機に接続される代理サーバ計算機から返送されたポート番号を識別し、当該ポート番号をクライアント計算機にかけて転送する手段とを備え、クライアント計算機は、サーバ計算機との間で、サーバ計算機のポート番号と、サーバ計算機に接続される代理サーバ計算機のポート番号とを交換する手段とを備える。

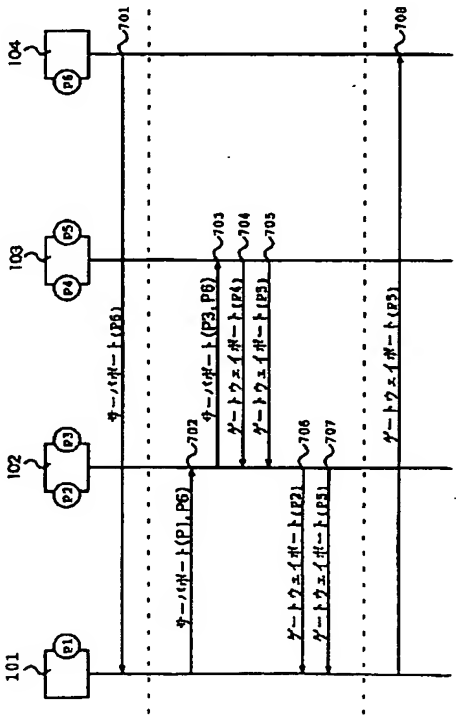



図9

【特許請求の範囲】
【請求項１】クライアント計算機と、サーバ計算機と、前記クライアント計算機およびサーバ計算機間の通信経路に介在し、個別にファイアウォールを構成する複数の代理サーバ計算機とを有し、前記通信経路上で、前記各計算機の通信アドレスおよび当該計算機で動的に割り振られるポート番号を指定してコネクションレス型の通信が行われるネットワーク通信システムであって、
前記各代理サーバ計算機は、前記サーバ計算機の通信アドレスおよび割り振ったポート番号を、前記クライアント計算機から、前記サーバ計算機に接続される前記代理サーバ計算機にかけて転送する手段と、当該転送に応じて、自代理サーバ計算機の通信アドレスおよび割り振ったポート番号を返送する手段と、前記サーバ計算機に接続される前記代理サーバ計算機から返送された通信アドレスおよび割り振ったポート番号を識別し、当該通信アドレスおよび割り振ったポート番号を前記クライアント計算機にかけて転送する手段とを備え、
前記クライアント計算機は、前記サーバ計算機との間で、当該サーバ計算機の通信アドレスおよび割り振ったポート番号と、前記サーバ計算機に接続される前記代理サーバ計算機の通信アドレスおよび割り振ったポート番号とを交換する手段とを備えることを特徴とするネットワーク通信システム。
【請求項２】請求項１記載のネットワーク通信システムであって、
前記クライアント計算機とサーバ計算機との間では、制御用コネクションを介して、通信アドレスおよび割り振ったポート番号の交換されることを特徴とするネットワーク通信システム。
【請求項３】クライアント計算機およびサーバ計算機間の通信経路に介在し、ファイアウォールを構成する代理サーバ計算機であって、
前記サーバ計算機の通信アドレスおよび割り振ったポート番号を、前記クライアント計算機側から、前記サーバ計算機に接続される前記代理サーバ計算機側に転送する手段と、当該転送に応じて、自代理サーバ計算機の通信アドレスおよび割り振ったポート番号を返送する手段と、前記サーバ計算機に接続される前記代理サーバ計算機から返送された通信アドレスおよび割り振ったポート番号を識別し、当該通信アドレスおよび割り振ったポート番号を前記クライアント計算機側に転送する手段とを備えることを特徴とする代理サーバ装置。
【請求項４】請求項１記載のネットワーク通信システムであって、
前記クライアント計算機および代理サーバ計算機は、前記通信経路上で接続される前記各計算機間で、相互認証を行うための手段を備えることを特徴とするネットワーク通信システム。
【請求項５】請求項１記載のネットワーク通信システムであって、
前記クライアント計算機および代理サーバ計算機は、前記クライアント計算機が前記各代理サーバ計算機と個別に相互認証を行うための手段を備えることを特徴とするネットワーク通信システム。
【請求項６】請求項４または５記載のネットワーク通信システムであって、
前記代理サーバ計算機は、前記相互認証の成立の可否に応じて、前記クライアント計算機の通信に対しアクセス制御を行う手段を備えることを特徴とするネットワーク通信システム。
【請求項７】請求項５記載のネットワーク通信システムであって、
前記クライアント計算機および代理サーバ計算機は、前記クライアント計算機と、前記サーバ計算機に直接接続される代理サーバ計算機との間で、前記相互認証に用いた暗号鍵を用いて通信の暗号化および復号化を行うための手段を備えることを特徴とするネットワーク通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、クライアント計算機およびサーバ計算機間の通信経路に、個別にファイアウォール（防火壁）を構成する複数の代理サーバが配置されているネットワークに係り、特に、クライアント計算機およびサーバ計算機間で、ポート番号の指定を伴ってコネクションレス型の通信が行われる通信システムに関する。
【０００２】
【従来の技術】ファイアウォールを構成する代理サーバを通信経路上に配置し、ポート番号と通信アドレスによりサービスを識別するトランスポート層において通信を中継する通信システムが提案されている。このトランスポート層の通信方式は、コネクション型通信と、コネクションレス型通信に大別される。
【０００３】コネクション型通信においては、転送先のポート番号が固定であり、かつ、通信開始時の転送元のポート番号も固定とされている。このため、中継経路を確立するために必要な情報を各通信装置が取得することが容易であった。
【０００４】しかし、コネクションレス型通信では、転送先のポート番号が動的にアサインされ、かつ、通信開始時の転送元のポート番号も不定であるため、通信経路を確立するために必要な情報を各通信装置が取得するのは難しい。
【０００５】従来、ファイアウォールが介在する環境下で、クライアント計算機とサーバ計算機との間でコネクションレス型通信を可能にする機能としては、RFC1928で提案されている Socks Protocol Version5 がある。Socks Protocol Version5 は、ファイアウォール上で通

信を中継する代理サーバと、代理サーバに対応した通信ライブラリにより構成されるシステムとを前提としたプロトコルであり、代理サーバとクライアント計算機の通信ライブラリとの間での相互認証を規定すると共に、クライアント計算機の代理サーバに対する接続命令およびその結果通知のシーケンスとパケットフォーマットとを規定している。

【０００６】コネクションレス型通信を行なうためには、クライアント計算機、サーバ計算機、代理サーバが、通信に使用するポート番号を互いに交換する必要がある。Socks Version5 のプロトコルでは、何らかの方法により、サーバ計算機からクライアント計算機に対して、サーバ計算機が通信に使用するポート番号を通知でき、逆に、クライアント計算機からサーバ計算機に対しては、サーバ計算機と通信を行なう代理サーバが使用するポートを通知できることを前提としている。その上で、Socks Version5 のプロトコルでは、クライアント計算機より代理サーバに、サーバ計算機の使用ポートを通知するための通信手順と、代理サーバよりクライアント計算機に、クライアント計算機とサーバ計算機の両方に対して代理サーバが中継で使用する２つのポートを通知するための通信手順とを提供する。

【０００７】例えば、クライアント計算機とサーバ計算機間の通信路上に、ファイアウォールを構成する代理サーバが一つだけ存在する場合には、図１４（ａ）に示すシーケンスにより、ポート番号の交換が行われる。すなわち、まず、サーバ計算機が、代理サーバとの通信に使用するポート番号Ｐ４をクライアント計算機に通知する。そのポート番号Ｐ４をクライアント計算機が代理サーバに通知し、代理サーバは、クライアント計算機との通信に使用するポート番号Ｐ２と、サーバ計算機との通信に使用するポート番号Ｐ３とをクライアント計算機に返送する。そして、クライアント計算機は、そのポート番号Ｐ３をサーバ計算機に通知する。

【０００８】

【発明が解決しようとする課題】しかしながら、従来技術である Socks Version5 のシーケンスでは、ファイアウォールを構成する代理サーバが通信経路上に複数個存在する場合には、うまくポート番号を交換することができない。

【０００９】通信経路上に２つの代理サーバ１および２が存在する場合には、例えば、図１４（ｂ）のように、まず、サーバ計算機が、代理サーバ２との通信に使用するポート番号Ｐ６をクライアント計算機に通知すると、そのポート番号Ｐ６は、代理サーバ１および２に順次通知される。そして、この通知に応じて、代理サーバ１は、自らが通信に使用する２つのポート番号Ｐ２およびＰ３をクライアント計算機に通知し、代理サーバ２も、通信に使用する２つのポート番号Ｐ４およびＰ５を代理サーバ１に通知する。ただし、代理サーバ２からの通知情報は、代理サーバ１のファイアウォールの機能により遮断される。そして、サーバ計算機には、コネクションレス型通信に必要なポート番号（Ｐ５）でなく、ポート番号Ｐ３が通知される。

【００１０】そこで、本発明では、計算機間の通信が、個別にファイアウォールを構成する複数の代理サーバにより中継される場合にも、ポート番号の交換およびコネクションレス型の通信を可能とするネットワーク通信システムを提供することを目的とする。

【００１１】

【課題を解決するための手段】上記課題を解決するために、本発明では、クライアント計算機と、サーバ計算機と、前記クライアント計算機およびサーバ計算機間の通信経路に介在し、個別にファイアウォールを構成する複数の代理サーバ計算機とを有し、前記通信経路上で、前記各計算機の通信アドレスおよび当該計算機で動的に割り振られるポート番号を指定してコネクションレス型の通信が行われるネットワーク通信システムであって、前記各代理サーバ計算機は、前記サーバ計算機の通信アドレスおよび割り振ったポート番号を、前記クライアント計算機から、前記サーバ計算機に接続される前記代理サーバ計算機にかけて転送する手段と、当該転送に応じて、自代理サーバ計算機の通信アドレスおよび割り振ったポート番号を返送する手段と、前記サーバ計算機に接続される前記代理サーバ計算機から返送された通信アドレスおよび割り振ったポート番号を識別し、当該通信アドレスおよび割り振ったポート番号を前記クライアント計算機にかけて転送する手段とを備え、前記クライアント計算機は、前記サーバ計算機との間で、当該サーバ計算機の通信アドレスおよび割り振ったポート番号と、前記サーバ計算機に接続される前記代理サーバ計算機の通信アドレスおよび割り振ったポート番号とを交換する手段とを備えることを特徴とするネットワーク通信システムを提供する。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態を、図１から図１３を用いて説明する。

【００１３】図１は、本実施形態に係るネットワーク通信システムの概要を示す図である。図１において、101はクライアント計算機、102と103は個別にファイアウォールを構成する代理サーバ、104はサーバ計算機、105と106はファイアウォールにより守られたネットワークドメイン、107と108はローカルセグメント、109はインターネットである。本例の各代理サーバ102および103は、認証およびアクセス制御の機能を備え、個別にファイアウォールを実現している。なお、代理サーバの機能を限定し、代理サーバを含む複数の計算機により一つのファイアウォールを実現するようにしてもよい。

【００１４】クライアント計算機102とサーバ計算機104との間の通信は、ローカルセグメント107のＬＡＮ、代

理サーバ102、インターネット109、代理サーバ103、および、ローカルセグメント108のＬＡＮを介して行われる。この通信では、コネクション型とコネクションレス型の２種類の通信方式が利用される。各計算機101～104は、予め定められたポート番号を使用してコネクション型通信を行うことができる。また、通信アドレスと、各コネクションで動的に割り振られたポート番号とを指定してコネクションレス型通信を行うことができる。

【００１５】クライアント計算機102とサーバ計算機104との間の通信では、まず、コネクション型通信により通信経路上の各計算機間でポート番号および通信アドレスの交換がなされる。以後、通信経路上の各計算機は、取得したポート番号および通信アドレスを指定してコネクションレス型通信によりパケットの通信を行う。なお、本例では通信経路上に代理サーバを２個配置しているが、３個以上配置した場合にも、同じ手順で通信がなれる。ポート番号の交換で使用されるコネクションの内、クライアント計算機101およびサーバ計算機104間の通信のコネクションだけは、制御用コネクションが用いられる。

【００１６】図２は、クライアント計算機102の構成例を示す図である。図において、クライアント計算機102は、ＣＰＵ23、メモリ21、外部記憶装置24、通信Ｉ／Ｏ25、および、バス22を有する。なお、図示はしないが、表示装置やキーボード、音声再生回路等の各種入出力装置と、通信データの暗号化／復号のためのプログラムや回路も備えている。

【００１７】外部記憶装置24には、通信プログラム241、データグラム中継制御プログラム242、中継経路テーブル243、認証情報テーブル244、および、各種アプリケーションプログラム（図示せず）が格納されている。通信プログラム241およびデータグラム中継制御プログラム242は、コネクション型通信によるポート番号の交換と認証とコネクションレス型通信とを行うためのプログラムである。中継経路テーブル243には、他のドメインの識別情報やそこへの通信に用いる通信アドレス、ポート番号等が含まれる。認証情報テーブル244には、図５に示すように、代理サーバ102のＩＤと、代理サーバ102と共有する認証用共有鍵1201とが記録される。なお、アプリケーションプログラムには、例えば、受信した動画像データや音声データをリアルタイムに再生する処理を行うもの等が含まれる。

【００１８】メモリ21には、中継経路情報記憶エリア211、通信データ記憶エリア212、プログラムロードエリア213、および、ポート情報記録テーブル214が形成されている。中継経路情報記憶エリア211には上記中継経路テーブル243の情報がロードされ、プログラムロードエリア213には上記外部記憶装置24内の各種プログラムがロードされる。ポート情報記録テーブル214は、図４（ａ）において、クライアント計算機101と接続する代理サーバ（102）の使用ポート番号および通信アドレスを記録するためのポート情報エリア2141と、サーバ計算機104と接続する代理サーバ（103）の使用ポートおよび通信アドレスを記録するためのポート情報エリア2142とにより構成される。

【００１９】ＣＰＵ23は、プログラムロードエリア213のプログラムを実行し、通信Ｉ／Ｏ25を用いてパケットの送受信を行う。通信の開始時、送信先は中継経路情報記録エリア211で検索する。送受信するパケットのデータは、通信データ記録エリア212に格納され、コネクション型通信により取得したポート番号および通信アドレスは、ポート情報記録エリア214に格納される。

【００２０】サーバ計算機104は、基本的にクライアント計算機と同様の構成を有するが、さらに、クライアント計算機に対し各種サービスを提供するためのアプリケーションプログラムやデータベース等を有する。ライアント計算機に提供するサービスとしては、例えば、動画像データや音声データの提供が含まれる。これらのデータは、データの信頼性よりもリアルタイムな転送が要求されるため、コネクションレス型通信に適している。

【００２１】図３は、個別にファイアウォールを形成する代理サーバ（102および103）の構成例を示す図である。図において、代理サーバは、ＣＰＵ33、メモリ31、外部記憶装置34、通信I/036、および、バス32を有する。通信データの暗号化／復号のためのプログラムや回路を備えることもできる。

【００２２】外部記憶装置34には、代理サーバプログラム341、中継経路テーブル342、認証情報テーブル343、および、アクセス制御テーブル344が格納されている。代理サーバプログラム341は、コネクション型通信によるポート番号の交換と認証およびアクセス制御と、コネクションレス型通信とを行うためのプログラムである。中継経路テーブル342には、他のドメインの識別情報やそこへの通信に用いる通信アドレス、ポート番号等が含まれる。

【００２３】認証情報テーブル343には、隣接する計算機のＩＤと、その計算機と共有する認証用共有鍵とが記録される。代理サーバ102の場合、図５に示すように、クライアント計算機101のＩＤ（ｃ１１）と認証用共有鍵1201とからなるエントリ34311と、代理サーバ103の識別情報（ｆｗ２）と認証用共有鍵1202とからなるエントリ34312とが記録される。アクセス制御テーブルは、図６において、ユーザＩＤが記録されるフィールド3441と、受信元アドレスが記録されるフィールド3442と、受信元のポート番号が記録されるポートフィールド3443とからなる。

【００２４】メモリ31には、中継経路情報記憶エリア311、通信データ記憶エリア312、プログラムロードエリア313、および、ポート情報記録テーブル314が形成されている。中継経路情報記憶エリア311には、上記中継経路

テーブル342の情報がロードされ、プログラムロードエリア313には、代理サーバプログラム341等のプログラムがロードされる。ポート情報記録テーブル314は、図４（ｂ）に示すように、クライアント計算機側の接続相手の使用ポート番号および通信アドレスを記録するためのポート情報エリア3141と、サーバ計算機側の接続相手の使用ポート番号および通信アドレスを記録するためのポート情報エリア3142とにより構成される。

【００２５】ＣＰＵ33は、プログラムロードエリア313のプログラムを実行し、通信Ｉ／Ｏ25を用いてパケットの送受信を行う。通信の開始時、送信先は中継経路情報記録エリア311で検索する。また、送受信するパケットのデータは、通信データ記録エリア312に格納され、コネクションレス型通信のためのポート番号は、ポート情報記録テーブル314に格納される。

【００２６】次に、クライアント計算機101がサーバ計算機104に対して通信を行なう際に、通信経路上の各計算機で行われる処理について説明する。

【００２７】図７は、サーバ計算機104との通信を行う際に、通信用のプログラムに基づいてクライアント計算機101で実施される処理の概要を示すフローチャートである。

【００２８】クライアント計算機101の通信用のプログラムでは、まず、サーバ計算機104でコネクション型通信用にアサインされたポート番号と通信アドレスとを、コネクション型通信の制御用コネクションによりサーバ計算機104から取得する（ステップ501）。次に、自計算機101のコネクションレス型通信用のポート番号をアサインし、上記取得したポート番号をポート情報エリア2142に格納する（ステップ502）。そして、代理サーバによる中継を必要とするかどうか判定し（ステップ503）、中継が不要な場合には、サーバ計算機104への接続を直接行なう（ステップ509）。

【００２９】中継が必要な場合は、ステップ509の代わりに次のステップ504から507の処理を行う。まず、サーバ計算機104への中継を行なう代理サーバ（102）を、中継経路テーブル243を参照して特定し（ステップ504）、その代理サーバ上で稼働している代理サーバプログラム341と接続する（ステップ505）。そして、ステップ501で取得したサーバ計算機104の通信アドレスおよびポート番号を、接続した代理サーバプログラム341に送信する（ステップ506）。次に、接続した代理サーバでアサインされたポート番号を、同代理サーバプログラム341より受けとり、ポート情報記録エリア2141に記録する（ステップ507）。さらに、サーバ計算機104に接続される代理サーバ（103）の代理サーバプログラム341の使用ポート番号を受けとり、ポート情報記録エリア2142に記録する（ステップ508）。

【００３０】次に、ポート情報記録エリア2142に記録した使用ポート番号および通信アドレスを、上記制御用コネクションによりサーバ計算機104に通知する（ステップ510）。そして、以後、ポート情報記録エリア2141に記録されている接続相手のポート番号および通信アドレスを指定して、サーバ計算機104との間でコネクションレス型のパケット通信を行う（ステップ511）。

【００３１】なお、以上のフローは、クライアント計算機101で動作するすべての通信プログラム241で共通しており、例えばUNIXOSの場合には、通信用ライブラリに上記機能を組み込むことができる。

【００３２】図８は、クライアント計算機101がサーバ計算機104と通信を行なう際に、それを中継する代理サーバで代理サーバプログラム342に基づいて実施される中継処理の概略を示すフローチャートである。

【００３３】代理サーバプログラム342は、まず、クライアント計算機もしくは他の代理サーバからの中継要求を待ち（ステップ601）、中継要求を送る通信相手と接続して、サーバ計算機104の通信アドレスおよびポート番号を取得する（ステップ602）。次に、クライアント側およびサーバ側の各接続相手のそれぞれついて、コネクションレス型通信用のポート番号をアサインする（ステップ603）。そして、サーバ計算機103との通信で他の代理サーバの中継を必要とするかどうかを判定する（ステップ604）。

【００３４】他の代理サーバの中継を必要とする場合、次のステップ605から611, 615の処理を行う。まず、サーバ計算機104への中継を行なう他の代理サーバ（代理サーバ102から見た場合、代理サーバ103）を、中継経路テーブル343を参照して特定し（ステップ605）、特定した代理サーバで稼働されている代理サーバプログラム341と接続する（ステップ606）。そして、ステップ602で取得したサーバ計算機104の通信アドレスおよびポート番号を、ステップ606で接続した代理サーバプログラム341に送信する（ステップ607）。送信先の代理サーバプログラム341からは、その代理サーバプログラム341がクライアント側の接続相手（つまり、自代理サーバ）に対してアサインしたポート番号と通信アドレスとを受けとり、ポート情報記録エリア3142に記録する（ステップ608）。さらに、同代理サーバプログラム341から、サーバ計算機104に接続される代理サーバ（103）がサーバ計算機104に対しアサインしたポート番号と通信アドレスとを受けとり、ポート情報記録エリア3411に記録する（ステップ609）。この２つのステップ608および609で受け取る情報は、自代理サーバプログラム341において、上記中継要求に対する応答であると認識され、他の外部からの情報とは区別される。認識を可能とするため、受け取る情報には例えば応答を示す識別子が含まれる。次に、ステップ601で接続した代理サーバもしくはクライアント計算機101に対し、ステップ603でアサインした同接続相手用のポート番号を送信し（ステップ610）、さらに、ステップ609で記録したサーバ計算機104用のポー

ト番号を送信する（ステップ611）。そして、以後、ポート情報記録テーブル314に記録されたポート番号および通信アドレスを指定して送られてくるパケットは、同テーブル314を基に、ポート番号および通信アドレスの書き替えを行って、コネクションレス型通信により転送する（ステップ615）。

【００３５】上記ステップ604で他の代理サーバによる中継が不要であると判定された場合（すなわち、サーバ計算機104に自代理サーバが接続する場合）には、次のステップ612から615の処理を行う。まず、ステップ602で取得したサーバ計算機のポート番号を、ポート情報記録エリア3142に記録する（ステップ612）。ステップ601で接続した相手用に自代理サーバがアサインしたポート番号を、同接続相手に送信する（ステップ613）。そして、ステップ603でサーバ計算機104用にアサインしたポート番号を、ステップ601で接続した相手に送信する（ステップ614）。そして、以後、上述のステップ615の処理によりパケットの転送を行う。

【００３６】さて、本ネットワーク通信システムでは、計算機間の相互認証と、代理サーバでのアクセス制御とを実施することにより、セキュリティを強化することができる。相互認証の方法としては、例えばISO／IEC9798認証を用いることができる。

【００３７】各計算機101～104間の相互認証の処理は、複数のステップからなり、各計算機間の接続時に行われる。クライアント計算機101と代理サーバ102との間の認証処理は、図７のフローではステップ505の時点、図８のフローではステップ602の時点で行われる。具体的には、図５の例では、まず、代理サーバ102は、自計算機のＩＤ（ｆｗ１）と乱数をクライアント計算機101へ送信する。クライアント計算機101は、受け取ったＩＤを基に、認証情報テーブル2441に予め格納されている代理サーバ102と共有する認証用共有鍵1201を取り出し、その認証用共有鍵1201を用いて、受け取った乱数を暗号化する。そして、暗号化した乱数と自計算機のＩＤ（ｃ１１）とを代理サーバ102に返送する。代理サーバ102では、認証情報テーブル3431に予め格納されているクライアント計算機101と共有する認証用共有鍵1201を取り出し、その認証用共有鍵1201を用いて、受け取った暗号化された乱数を復号化する。そして、送信した乱数と復号化した乱数が一致した場合には認証成立とし、次の処理に進む。一致しない場合は、認証不成立としてコネクションを切断する。認証側と非認証側を逆にして以上の処理を繰り返すことで、相互認証がなされる。

【００３８】代理サーバ間の認証処理も、図８のステップ602および606の時点において同様に行われる。図５の例では、代理サーバ103が乱数を代理サーバ102に送信し、代理サーバ102は、受け取った乱数を、代理サーバ103と共有する認証用共有鍵1202を用いて暗号化し返送する。代理サーバ103では、代理サーバ103と共有する認証用共有鍵1202を用いて、受け取った暗号化された乱数を復号化し、送信した乱数と復号化した乱数が一致した場合のみ認証成立とする。ここでも、認証側と非認証側を逆にして同じ処理を繰り返すことで、相互認証がなされる。

【００３９】各代理サーバでのアクセス制御は、図８のステップ602の認証処理の直後に行う。アクセス制御のため、各代理サーバの代理サーバプログラムは、受信したパケットから、クライアント計算機102を使用しているユーザのユーザＩＤと通信アドレスを取得し、アクセス制御テーブル344に記録された情報と一致する場合のみ処理を続行する。

【００４０】図９は、上述のフローチャートの処理により実施される通信シーケンスの具体例を説明するための図である。

【００４１】図で、通信手順701～708は、それぞれ、１または複数のパケットによる通信を示す。Ｐ１からＰ５は、各計算機でコネクションレス型通信用にアサインされたポート番号を示す。サーバ計算機104は、代理サーバ104との通信用にポート番号Ｐ６アサインし、クライアント計算機101では、代理サーバ102との通信用にポート番号Ｐ１をアサインする。代理サーバ102は、クライアント計算機101との通信用にポート番号Ｐ２、代理サーバ103との通信用にポート番号Ｐ３をそれぞれアサインする。そして、代理サーバ103は、代理サーバ103との通信用にポート番号Ｐ４、サーバ計算機104との通信用にポート番号Ｐ５をアサインする。

【００４２】まず、通信手順701では、サーバ計算機104のポート番号Ｐ６および通信アドレスが、制御用コネクションによりサーバ計算機104からクライアント計算機101に通知される。通信手順702では、サーバ計算機104のポート番号Ｐ６および通信アドレスと、クライアント計算機101のポート番号Ｐ１および通信アドレスとが、通常のコネクションによりクライアント計算機101から代理サーバ102に通知される。同様に、通信手順703では、サーバ計算機104のポート番号Ｐ６および通信アドレスと、代理サーバ102のポート番号Ｐ３および通信アドレスとが、代理サーバ102から代理サーバ103に通知される。通信手順704および705では、代理サーバ103のポート番号Ｐ４およびＰ５と通信アドレスとが、代理サーバ103から代理サーバ102に通知される。通信手順706および707では、代理サーバ102のポート番号Ｐ２および通信アドレスと、代理サーバ103のポート番号Ｐ５および通信アドレスとが、代理サーバ102からクライアント計算機101に通知される。そして、通信手順708では、代理サーバ103のポート番号Ｐ５および通信アドレスが、制御用コネクションによりクライアント計算機101からサーバ計算機102に通知される。以上の手順により、各計算機102～104は、それぞれ、接続する計算機のポート番号および通信アドレスを獲得することができる。

【００４３】相互認証およびアクセス制御は、通信手順702および703において実施される。なお、アクセス制御については、逆方向の通信がなされる通信手順704および706において実施してもよい。また、相互認証およびアクセス制御は、通信手順701において行ってもよい。

【００４４】次に、本発明の他の実施形態について、図１０から図１３を用いて説明する。

【００４５】この実施形態に係るネットワーク通信システムは、クライアント計算機の通信用のプログラムによる処理と、代理サーバの中継プログラムによる処理とが、上述の実施形態と異なる。

【００４６】図１０は、サーバ計算機104と通信を行う際に、クライアント計算機101の通信用のプログラムにより実施される処理の概略を示すフローチャートである。

【００４７】クライアント計算機101の通信用のプログラムは、まず、サーバ計算機104でコネクション型通信用にアサインされたポート番号と通信アドレスとを、制御用コネクションによりサーバ計算機104から取得する（ステップ801）。次に、自計算機101のコネクションレス型通信用のポート番号をアサインし、上記取得したポート番号をポート情報エリア2142に格納する（ステップ802）。そして、代理サーバによる中継を必要とするかどうか判定し（ステップ803）、中継が不要な場合には、サーバ計算機104への接続を直接行なう（ステップ813）。

【００４８】中継が必要な場合は、ステップ813の代わりに次のステップ804から812の処理を行う。まず、サーバ計算機104への中継を行なう代理サーバ（102）を、中継経路テーブル243を参照して特定し（ステップ804）、その代理サーバ上で稼働している代理サーバプログラム341と接続する（ステップ805）。そして、ループカウンタをリセットする（ステップ806）。

【００４９】次に、上記接続した代理サーバプログラム341に対し、ステップ801で取得したサーバ計算機104の通信アドレスおよびポート番号を送信する（ステップ807）。そして、上記接続した代理サーバプログラム341からポート番号および通信アドレスを受け取る（ステップ820）。この際、この情報の生成元が、サーバ計算機104に接続する代理サーバである場合には、接続完了情報も受け取る。次に、ループカウンタの値が０値かどうかを判定し（ステップ808）、０値の場合には、上記受け取ったポート番号をポート情報記録エリア2141に記録する（ステップ809）。次に、上記ステップ820で受け取ったポート番号をポート情報記録エリア2142に記録し（ステップ810）、ループカウンタの値をインクリメントする（ステップ811）。そして、接続完了情報の受け取りの有無により、サーバ計算機104に接続する代理サーバとの接続が完了したかどうかを判定し（ステップ812）、完了していない場合には、上記ステップ807以降の処理を繰り返す。

【００５０】接続が完了した場合には、ポート情報記録エリア2142のポート番号を、制御用コネクションによりサーバ計算機104に通知する（ステップ814）。そして、以後、ポート情報記録エリア2141に記録されている接続相手のポート番号および通信アドレスを指定して、サーバ計算機104との間でコネクションレス型のパケット通信を行う（ステップ815）。

【００５１】図１１は、クライアント計算機101がサーバ計算機104と通信を行なう際に、それを中継する代理サーバで代理サーバプログラム342に基づいて実施される中継処理の概略を示すフローチャートである。

【００５２】代理サーバプログラム342は、まず、クライアント計算機もしくは他の代理サーバからの中継要求を待ち（ステップ901）、中継要求を送る通信相手と接続して、サーバ計算機104の通信アドレスおよびポート番号を受け取る（ステップ902）。さらに、接続相手の通信アドレスおよびポート番号を受け取り、ポート情報記録エリア3141に記録する（ステップ903）。次に、クライアント側およびサーバ側の各接続相手について、コネクションレス型通信用のポート番号をアサインし（ステップ904）、サーバ計算機103との通信で他の代理サーバの中継を必要とするかどうかを判定する（ステップ905）。

【００５３】他の代理サーバの中継を必要とする場合、次のステップ906から917の処理を行う。まず、サーバ計算機104への中継を行なう他の代理サーバ（代理サーバ102から見た場合、代理サーバ103）を、中継経路テーブル343を参照して特定し（ステップ906）、特定した代理サーバ103で稼働されている代理サーバプログラム341と接続する（ステップ907）。そして、ループカウンタをリセットする（ステップ908）。

【００５４】次に、クライアント計算機101から送られた情報（中継要求）を、上記ステップ907で接続した代理サーバに転送する（ステップ909）。そして、その代理サーバからは、その代理サーバが本代理サーバとの通信に対しアサインしたポート番号と通信アドレスとを受け取り（ステップ910）、さらに、その代理サーバがサーバ計算機104側の通信に対しアサインしたポート番号と通信アドレスとを受け取る（ステップ911）。この２つのステップ910, 911で受け取る情報は、上記中継要求に対する応答であると認識され、他の外部からの情報とは区別される。認識を可能とするため、受け取る情報には、例えば、応答を示す識別子が含まれる。次に、ループカウンタの値が０値かどうかを判定し（ステップ912）、０値の場合には、上記ステップ910で受け取ったポート番号および通信アドレスをポート情報記録エリア3141に記録する（ステップ913）。次に、同ポート番号および通信アドレスを、上記ステップ901で接続した相手に送信し（ステップ915）、ループカウンタの値をイン

クリメントする（ステップ916）。そして、接続完了情報の受け取りの有無により、サーバ計算機104に接続する代理サーバとの接続が完了したかどうかを判定し（ステップ917）、完了していない場合には、上記ステップ909以降の処理を繰り返す。

【００５５】接続が完了した場合には、以後、ポート情報記録テーブル314に記録されたポート番号および通信アドレスを指定して送られてくるパケットは、同テーブル314を基に、ポート番号および通信アドレスの書き替えを行って、コネクションレス型通信により転送する。

【００５６】上記ステップ905で他の代理サーバによる中継が不要であると判定された場合には、次のステップ918から921の処理を行う。まず、ステップ902で取得したサーバ計算機のポート番号を、ポート情報記録エリア3142に記録する（ステップ918）。ステップ901で接続した相手用に自代理サーバがアサインしたポート番号を、同接続相手に送信する（ステップ919）。そして、ステップ904でサーバ計算機104用にアサインしたポート番号を、ステップ901で接続した相手に送信する（ステップ920）。そして、以後、上述のステップ921の処理によりパケットの転送を行う。

【００５７】本実施形態においても、先の実施形態と同様のステップから実現される相互認証およびアクセス制御を実施することにより、セキュリティを強化することができる。ただし、本実施形態では、クライアント計算機101と各代理サーバとの間で、相互認証およびアクセス制御がなされる点が異なる。このため、クライアント計算機101は、図１２に示すように、認証用の共有鍵1203を代理サーバ102と共有し、これとは異なる共有鍵1204を代理サーバ103と共有する。そして、対象の代理サーバと共有する共有鍵を用いて認証処理を行う。相互認証の処理は、図１０のフローではステップ807～812が形成する処理ループにおいて、図１１のフローではステップ902において、それぞれ実施される。アクセス制御の処理は、図１１のステップ902の認証処理の直後に行われる。各代理サーバは、クライアント計算機102との相互認証およびアクセス制御が成立した場合に限り、クライアント計算機102と他の代理サーバとの間の通信を中継する。

【００５８】図１３は、以上本実施形態のフローチャートの処理により実現される通信シーケンスの具体例を説明するための図である。この図では、上述の図９と同じ値のポート番号Ｐ１からＰ６が各計算機101～104でアサインされる場合を示している。

【００５９】まず、通信手順1001により、サーバ計算機104のポート番号Ｐ６および通信アドレスが、サーバ計算機104からクライアント計算機101に通知される。クライアント計算機101は、通知されたポート番号Ｐ６および通信アドレスと、自計算機のポート番号Ｐ１および通信アドレスとを、通信手順1002により代理サーバ102に通知し、逆に、代理サーバ102からは、通信手順1003および1004により代理サーバ102の通信アドレスとポート番号Ｐ２およびＰ３の通知を受ける。次の通信手順1005では、クライアント計算機101がサーバ計算機104のポート番号Ｐ６および通信アドレスと、自計算機のポート番号Ｐ１および通信アドレスとを再び送信し、この情報は代理サーバ103で中継されて代理サーバ103に通知される。そして、代理サーバ103は、通信手順1006および1007で、自らの通信アドレスとポート番号Ｐ４およびＰ５を送信する。この送信情報は、代理サーバ102で中継され、通信手順1008および1009により、クライアント計算機101へ通知される。以上の手順により、各計算機102～104は、それぞれ、接続する計算機のポート番号および通信アドレスを獲得することができる。

【００６０】相互認証およびアクセス制御は、通信手順1002においてクライアント計算機101と代理サーバ102の間での相互認証を、通信手順1005においてクライアント計算機101と代理サーバ103の間での相互認証を行う。さらに、代理サーバ102が、通信手順1002での認証結果に応じてクライアント計算機101の通信のアクセス制御を行ない、代理サーバ103も、通信手順1005での認証結果に応じてクライアント計算機101の通信のアクセス制御を行なう。このように、相互認証およびアクセス制御を行うことで、セキュリティーをより高めることができる。

【００６１】コネクションレス型通信への移行後、クライアント計算機101と、サーバ計算機に接続される代理サーバ（103）との間の通信では、相互認証に用いた共有暗号鍵1204を利用して、通信データの暗号化および復号を行うようにすることができる。すなわち、送信側で暗号化を行い、受信側でその復号を行うことで、セキュリティーをさらに強化することができる。

【００６２】

【発明の効果】以上で説明したように、本発明によれば、計算機間の通信が、個別にファイアウォールを構成する複数の代理サーバにより中継される場合にも、ポート番号の交換およびコネクションレス型の通信を可能とするネットワーク通信システムを提供することができる。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るネットワーク通信システムの全体構成図。

【図２】　クライアント計算機の構成図。

【図３】　代理サーバ計算機の構成図。

【図４】　ポート情報記録テーブルの構成図。

【図５】　認証情報テーブルの構成および認証処理の説明図。

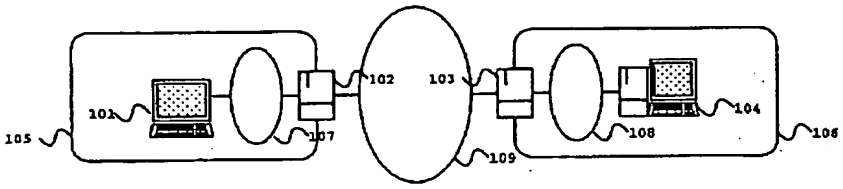
【図６】　アクセス制御テーブルの構成図。

【図７】　クライアント計算機の通信プログラムの概略フロー。

【図８】　代理サーバの通信プログラムの概略フロー。
【図９】　通信シーケンスの具体例。
【図１０】　クライアント計算機の通信プログラムの概略フロー(その2)。
【図１１】　代理サーバの通信プログラムの概略フロー(その2)。
【図１２】　認証情報テーブルの構成および認証処理の説明図（その２）。
【図１３】　通信シーケンスの具体例(その2)。
【図１４】　従来のシステムにおける問題点の説明図。
【符号の説明】
101...クライアント計算機、102...ファイアウォール（代理サーバ）、103...ファイアウォール（代理サーバ）、104...サーバ計算機、105...ネットワークドメイン、106...ネットワークドメイン、107...ローカルセグメント、108...ローカルセグメント、109...インターネット、21...メモリ、211...中継経路情報記憶エリア、212...通信データ記憶エリア、213...プログラムロードエリア、214...ポート情報記録エリア、22...バス、23...CPU、24...外部記憶装置、241...通信プログラム、242...データグラム中継制御プログラム、243...中継経路テーブル、25...通信I/O、31...メモリ、311...中継経路情報記憶エリア、312...通信データ記憶エリア、313...プログラムロードエリア、314...ポート情報記録エリア、32...バス、33...CPU、34...外部記憶装置、341...代理サーバプログラム342...中継経路テーブル、35...通信I/O、36...通信I/O、2141...クライアント計算機101と通信する代理サーバ102の使用ポートを記録するポート情報エリア、2142...サーバ計算機104と通信する代理サーバ103の使用ポートを記録するサーバ用ポート情報エリア、3141...クライアント計算機側の通信相手の使用ポートを記録するポート情報エリア、3142...サーバ計算機側の通信相手の使用ポートを記録するポート情報エリア。

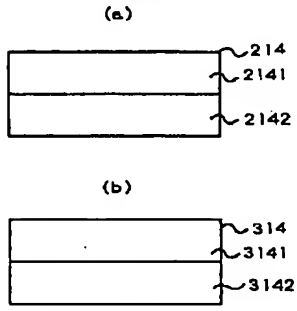
【図１】

図 1



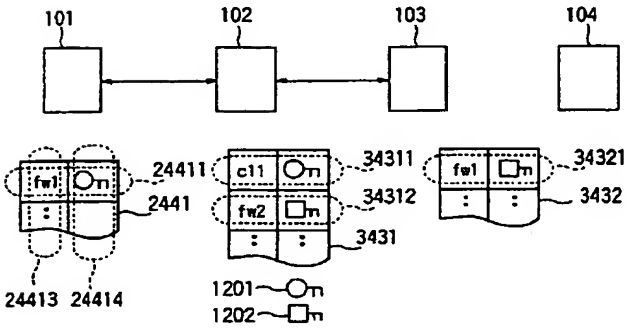

【図４】

図 4



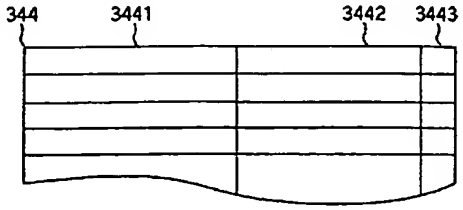

【図５】

図 5



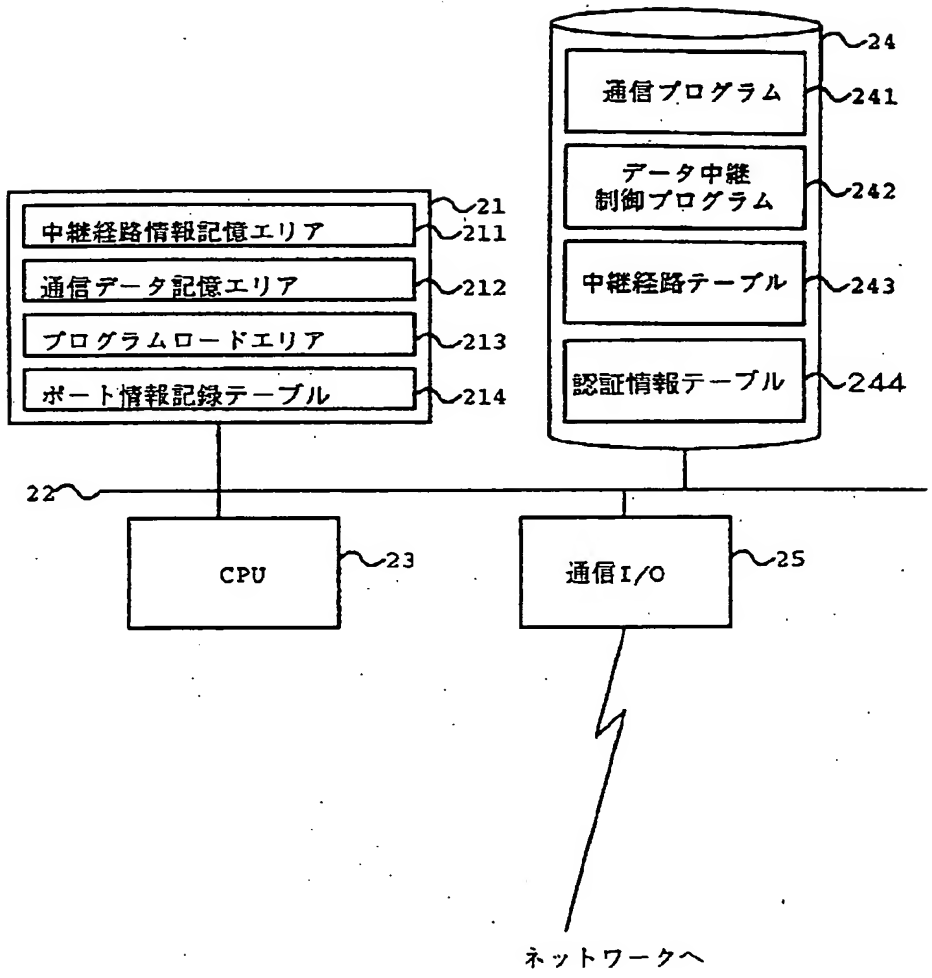

【図６】

図 6



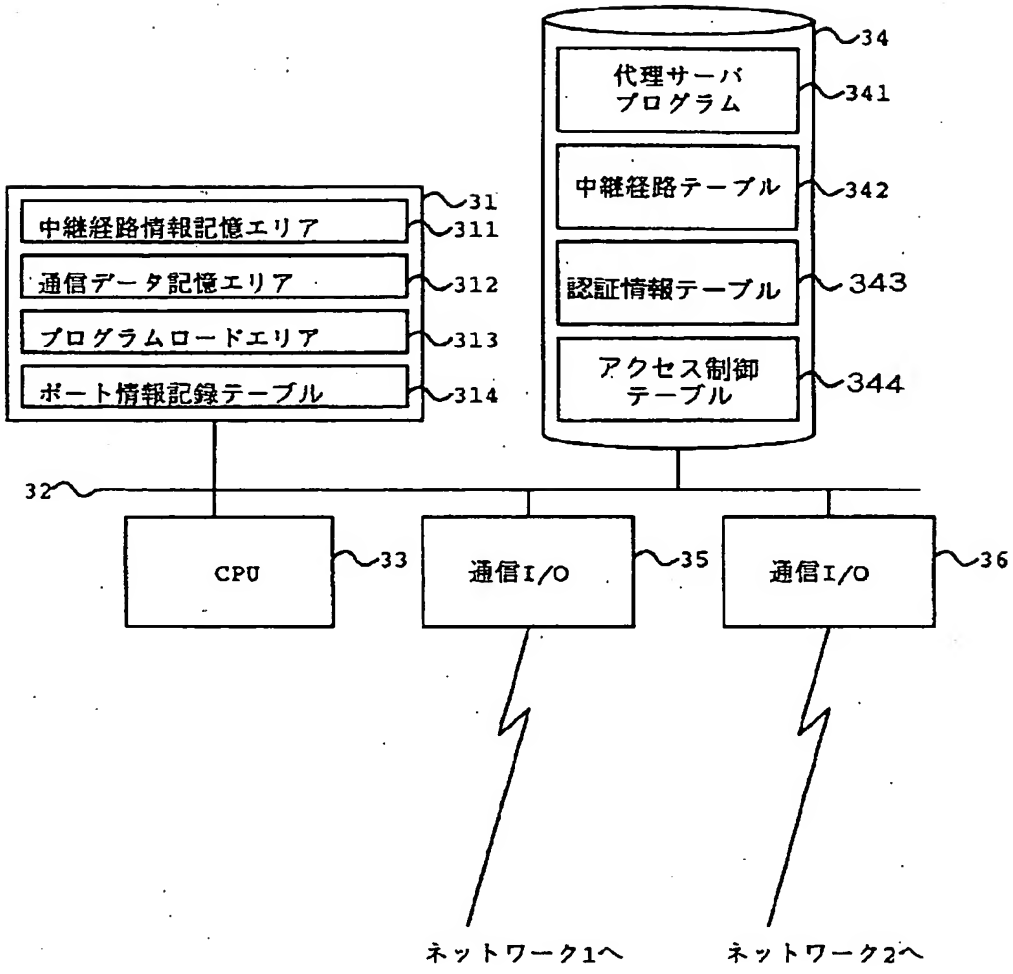
【図２】

図 2


24
通信プログラム
241
データ中継
制御プログラム
242
中継経路テーブル
243
認証情報テーブル
244
21
中継経路情報記憶エリア
211
通信データ記憶エリア
212
プログラムロードエリア
213
ポート情報記録テーブル
214
22
CPU
23
通信I/O
25
ネットワークへ

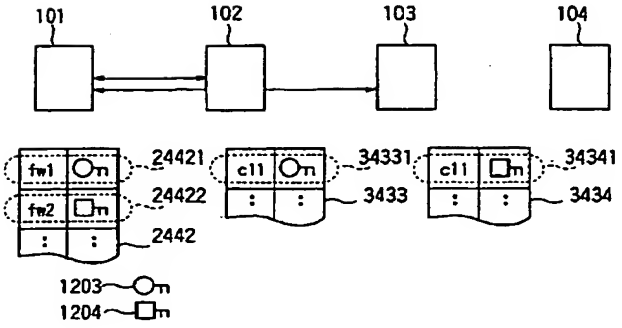
【図３】

図 3


34
代理サーバ
プログラム
341
中継経路テーブル
342
認証情報テーブル
343
アクセス制御
テーブル
344
31
中継経路情報記憶エリア
311
通信データ記憶エリア
312
プログラムロードエリア
313
ポート情報記録テーブル
314
32
CPU
33
通信I/O
35
通信I/O
36
ネットワーク1へ
ネットワーク2へ

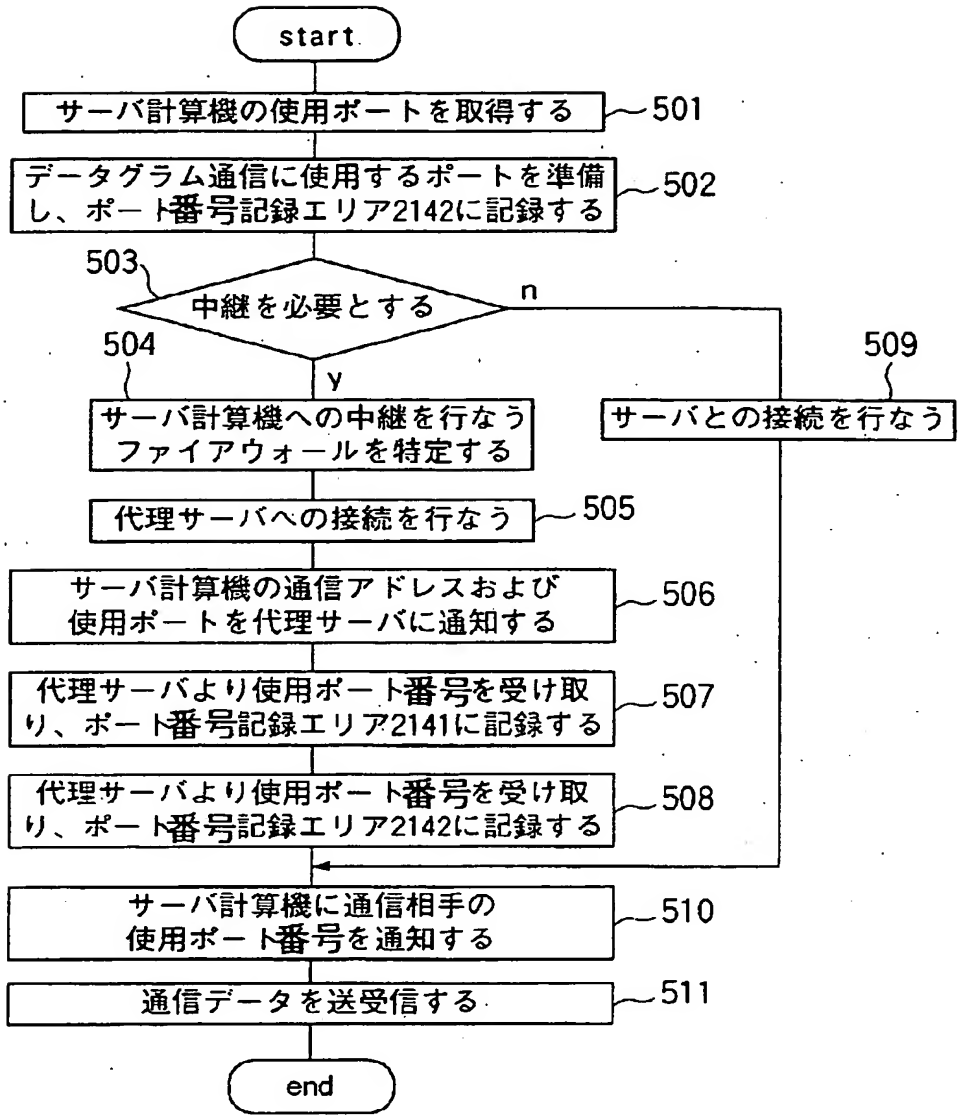
【図１２】

図12


101
102
103
104
fw1
fw2
24421
24422
2442
1203
1204
c11
34331
3433
c11
34341
3434

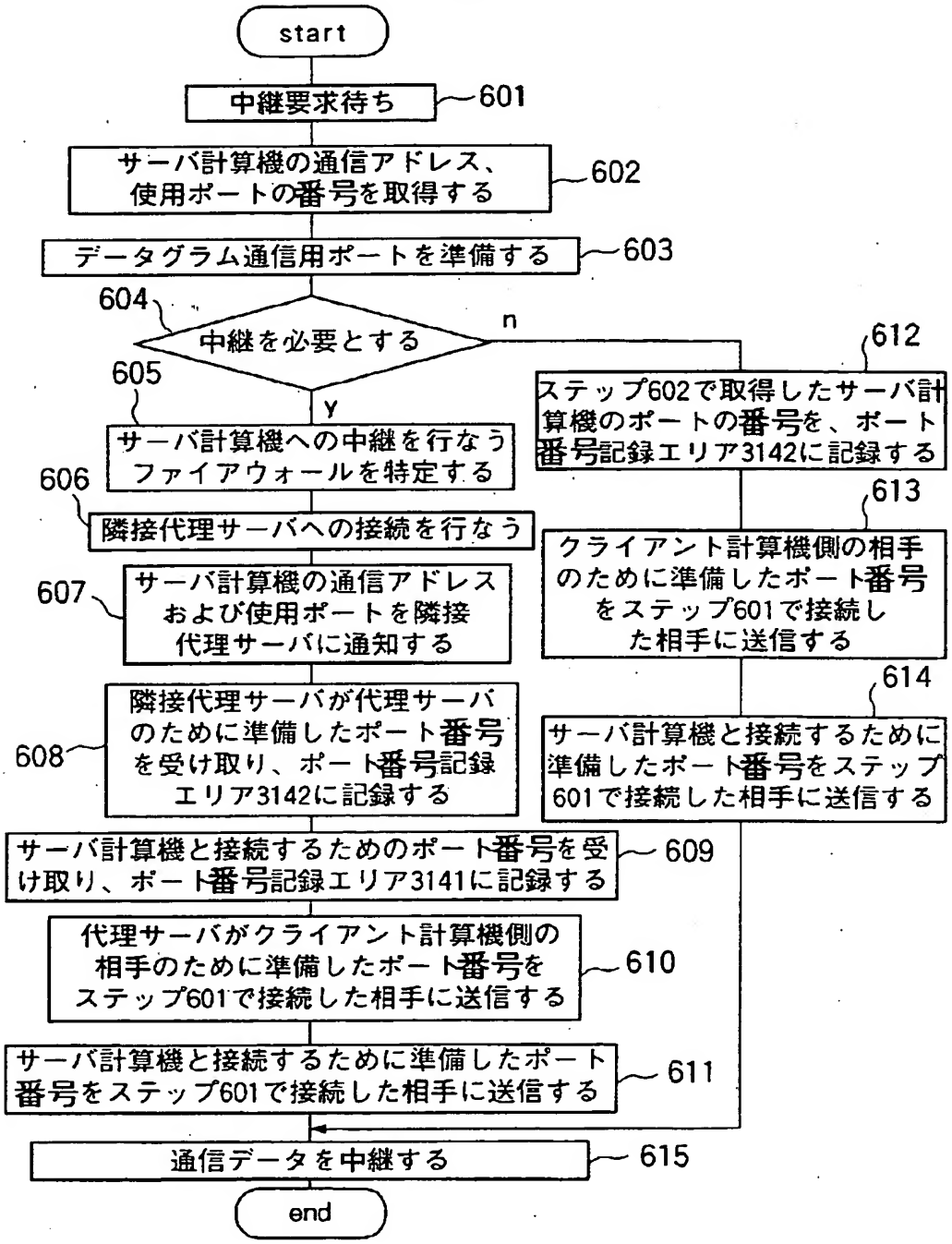
【図７】

図 7


start
サーバ計算機の使用ポートを取得する
501
データグラム通信に使用するポートを準備し、ポート番号記録エリア2142に記録する
502
503
中継を必要とする
n
504
y
509
サーバ計算機への中継を行なうファイアウォールを特定する
サーバとの接続を行なう
代理サーバへの接続を行なう
505
サーバ計算機の通信アドレスおよび使用ポートを代理サーバに通知する
506
代理サーバより使用ポート番号を受け取り、ポート番号記録エリア2141に記録する
507
代理サーバより使用ポート番号を受け取り、ポート番号記録エリア2142に記録する
508
サーバ計算機に通信相手の使用ポート番号を通知する
510
通信データを送受信する
511
end

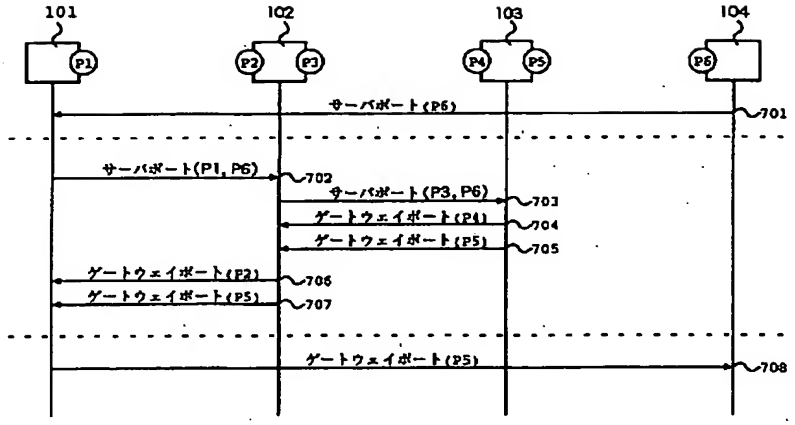
【図８】

図 8


start
中継要求待ち
601
サーバ計算機の通信アドレス、使用ポートの番号を取得する
602
データグラム通信用ポートを準備する
603
604
中継を必要とする
n
y
612
ステップ602で取得したサーバ計算機のポートの番号を、ポート番号記録エリア3142に記録する
605
サーバ計算機への中継を行なうファイアウォールを特定する
606
隣接代理サーバへの接続を行なう
613
クライアント計算機側の相手のために準備したポート番号をステップ601で接続した相手に送信する
607
サーバ計算機の通信アドレスおよび使用ポートを隣接代理サーバに通知する
614
サーバ計算機と接続するために準備したポート番号をステップ601で接続した相手に送信する
608
隣接代理サーバが代理サーバのために準備したポート番号を受け取り、ポート番号記録エリア3142に記録する
サーバ計算機と接続するためのポート番号を受け取り、ポート番号記録エリア3141に記録する
609
代理サーバがクライアント計算機側の相手のために準備したポート番号をステップ601で接続した相手に送信する
610
サーバ計算機と接続するために準備したポート番号をステップ601で接続した相手に送信する
611
通信データを中継する
615
end

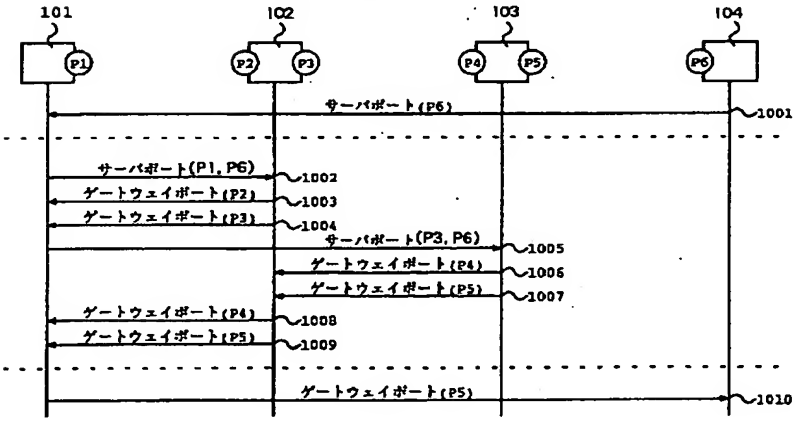
【図９】

図9


101
102
103
104
P1
P2
P3
P4
P5
P6
サーバポート(P6)
701
サーバポート(P1, P6)
702
サーバポート(P3, P6)
703
ゲートウェイポート(P4)
704
ゲートウェイポート(P5)
705
ゲートウェイポート(P2)
706
ゲートウェイポート(P5)
707
ゲートウェイポート(P5)
708

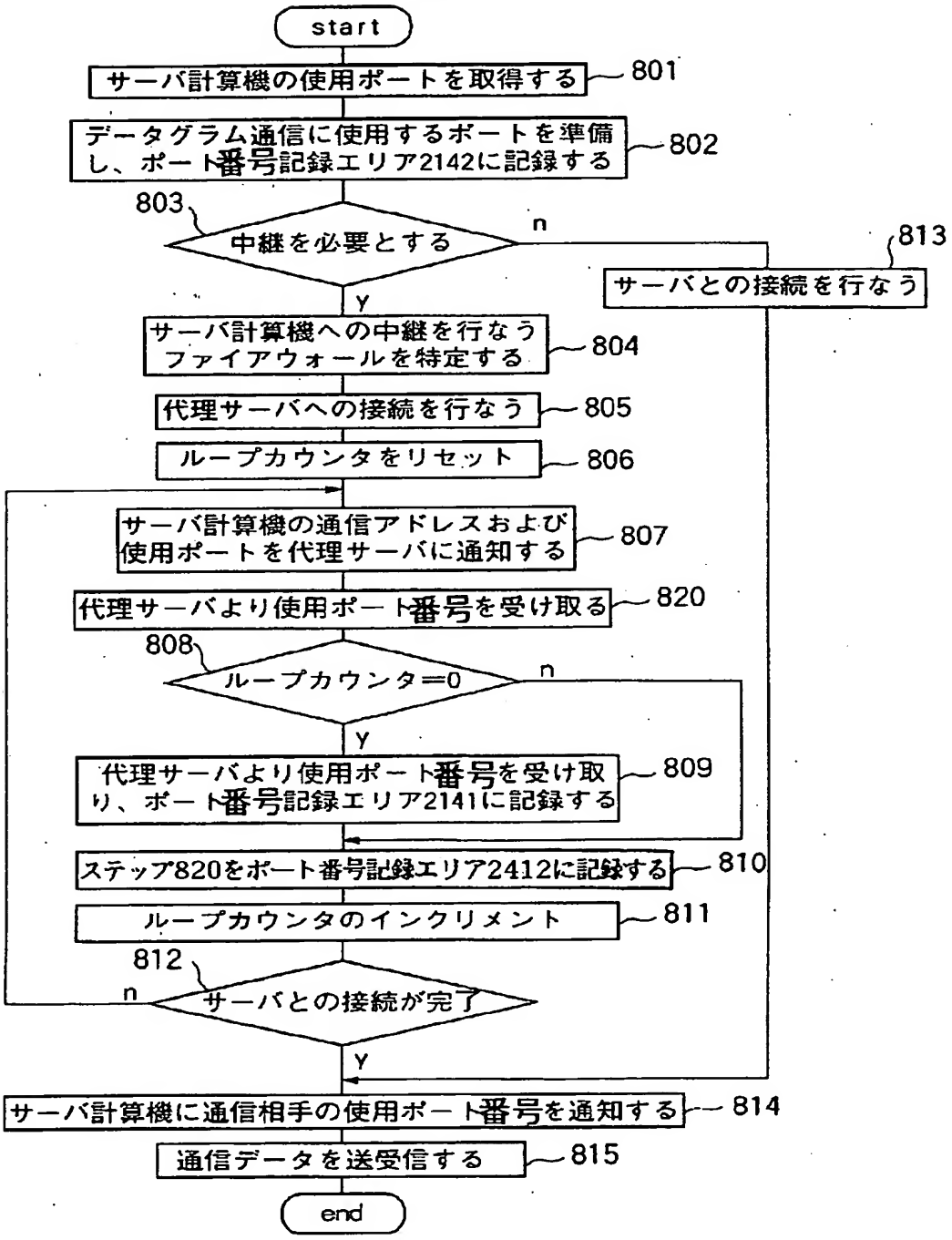
【図１３】

図１３


101
102
103
104
P1
P2
P3
P4
P5
P6
サーバポート(P6)
1001
サーバポート(P1, P6)
1002
ゲートウェイポート(P2)
1003
ゲートウェイポート(P3)
1004
サーバポート(P3, P6)
1005
ゲートウェイポート(P4)
1006
ゲートウェイポート(P5)
1007
ゲートウェイポート(P4)
1008
ゲートウェイポート(P5)
1009
ゲートウェイポート(P5)
1010

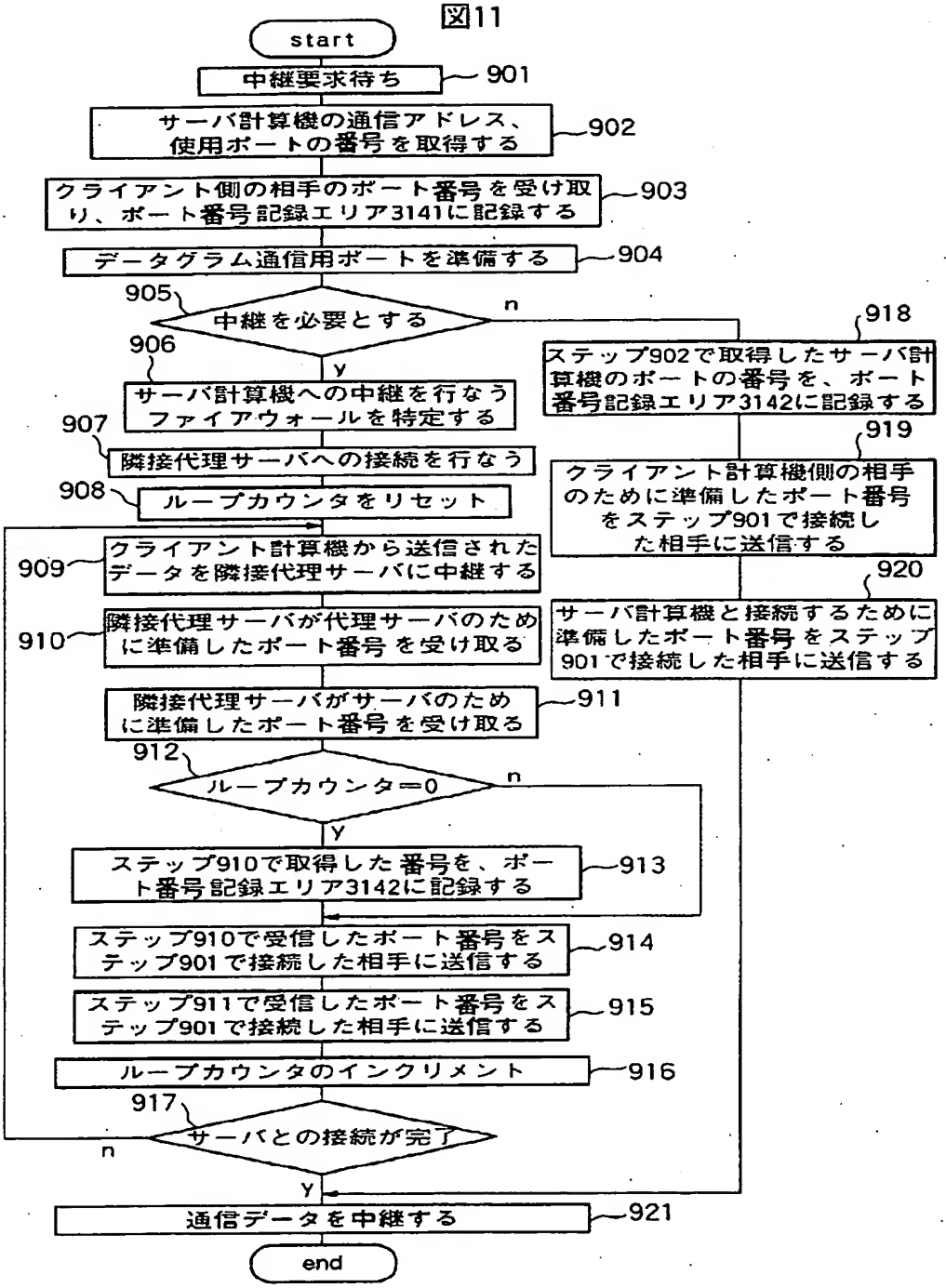
【図１０】

図10


start
サーバ計算機の使用ポートを取得する
801
データグラム通信に使用するポートを準備し、ポート番号記録エリア2142に記録する
802
803
中継を必要とする
n
813
サーバとの接続を行なう
Y
サーバ計算機への中継を行なうファイアウォールを特定する
804
代理サーバへの接続を行なう
805
ループカウンタをリセット
806
サーバ計算機の通信アドレスおよび使用ポートを代理サーバに通知する
807
代理サーバより使用ポート番号を受け取る
820
808
ループカウンタ=0
n
Y
代理サーバより使用ポート番号を受け取り、ポート番号記録エリア2141に記録する
809
ステップ820をポート番号記録エリア2412に記録する
810
ループカウンタのインクリメント
811
812
n
サーバとの接続が完了
Y
サーバ計算機に通信相手の使用ポート番号を通知する
814
通信データを送受信する
815
end

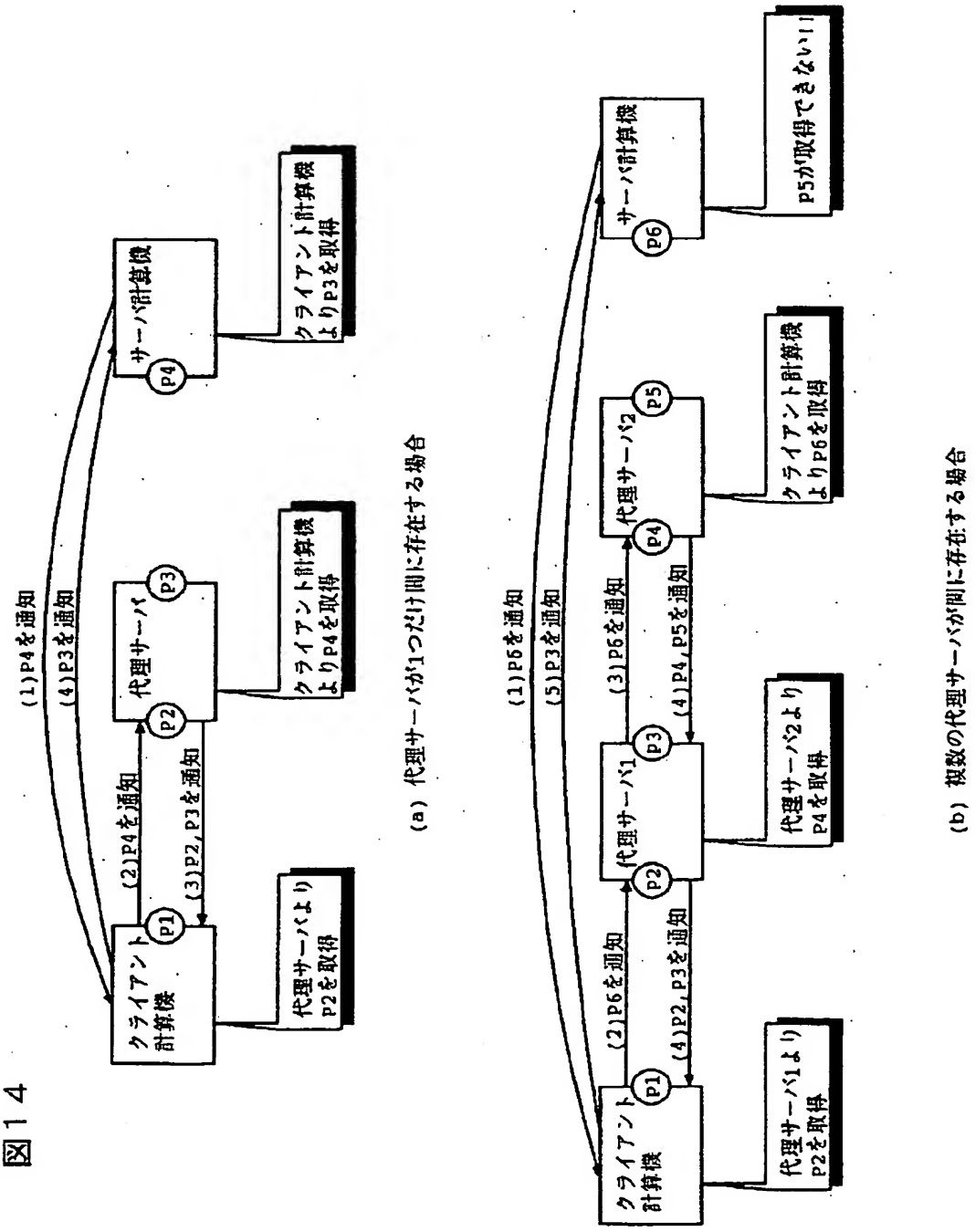
【図１１】

図11


start
中継要求待ち
901
サーバ計算機の通信アドレス、使用ポートの番号を取得する
902
クライアント側の相手のポート番号を受け取り、ポート番号記録エリア3141に記録する
903
データグラム通信用ポートを準備する
904
905
中継を必要とする
n
y
906
サーバ計算機への中継を行なうファイアウォールを特定する
907
隣接代理サーバへの接続を行なう
908
ループカウンタをリセット
909
クライアント計算機から送信されたデータを隣接代理サーバに中継する
910
隣接代理サーバが代理サーバのために準備したポート番号を受け取る
911
隣接代理サーバがサーバのために準備したポート番号を受け取る
912
ループカウンタ=0
n
y
913
ステップ910で取得した番号を、ポート番号記録エリア3142に記録する
914
ステップ910で受信したポート番号をステップ901で接続した相手に送信する
915
ステップ911で受信したポート番号をステップ901で接続した相手に送信する
916
ループカウンタのインクリメント
917
サーバとの接続が完了
n
y
921
通信データを中継する
end
918
ステップ902で取得したサーバ計算機のポートの番号を、ポート番号記録エリア3142に記録する
919
クライアント計算機側の相手のために準備したポート番号をステップ901で接続した相手に送信する
920
サーバ計算機と接続するために準備したポート番号をステップ901で接続した相手に送信する

【図１４】

図１４




フロントページの続き

(72)発明者　加藤　恵理
神奈川県横浜市戸塚区戸塚町5030番地　株
式会社日立製作所ソフトウェア開発本部内